IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF NEBRASKA

| | |
|---|---|
| UNITED STATES OF AMERICA,<br>Plaintiff,<br>vs.<br>KIRK COTTOM,<br>Defendant. | **8:13CR108**<br>**8:15CR239**<br><br>**MEMORANDUM AND ORDER** |

This matter is before the court after an evidentiary hearing on August 3, 2015, on the defendant's motion in limine, Filing No. 215.[1] This Memorandum and Order supplements findings made on the record at the hearing. *See* Filing No. 257, Transcript of August 3, 2015, hearing ("Hr'g Tr.") at 182-84.

I. BACKGROUND

The defendant was charged in the Second Superseding Indictment in Case No. 8:13CR108 with receipt and attempted receipt of child pornography (Count I), in violation of 18 U.S.C. § 2252A(a)(2) and (b)(1), and with accessing a computer in interstate commerce with the intent to view child pornography (Count II), in violation of 18 U.S.C. § 2252A(a)(5)(B), between November 18, 2012, and December 2, 2012, and in Case No. 8:15CR239 with receipt and attempted receipt of child pornography (Count I), in violation of 18 U.S.C. § 2252A(a)(2)(A) and (b)(1), and with accessing a computer in interstate commerce with the intent to view child pornography (Counts II-IV), between on or about February 1, 2013, and on or about April 9, 2013. The facts are set out in several other orders and will be repeated here only as necessary. *See* Filing No. 155, Memorandum and Order at 4-7; Filing No. 148, Findings and Recommendation ("F&R")

[1] The plaintiff also reasserts his earlier motion to suppress. *See* Filing No. 257, Hr'g Tr. at 161.

at 5-7. The defendant has entered into a conditional plea agreement, reserving the right to appeal the court's rulings on his motion to suppress and motion in limine. Filing No. 244, Plea Agreement.

This action involves an investigation of child pornography offenses that utilized the deployment, pursuant to a warrant, of a network investigative technique ("NIT") in order to obtain the IP addresses of persons who accessed a child pornography website that had been seized and was operated by the Federal Bureau of Investigation ("FBI") for several weeks in late 2012. The defendant, along with other defendants, challenged the NIT in a motion to suppress. Filing No. 53. The magistrate judge recommended that the motion be denied and this court overruled the defendant's objections to that recommendation and adopted the magistrate judge's findings. Filing No. 148, F&R; Filing No. 155, Memorandum and Order.

The record shows that in the course of these proceedings, the defendant moved for additional discovery, including the original source code that was used to create and deploy the NIT. The government concedes that the original source code was not preserved. The defendant seeks exclusion of the expert testimony of FBI Special Agents Steven A. Smith and Supervisory Special Agent P. Michael Gordon under *Daubert v. Merrell Dow Pharmaceuticals*, 509 U.S. 579 (1983). Filing No. 215. The defendant contends that the government's experts' opinions regarding the NIT employed in this case lack proper foundation and are based on insufficient data. He contends his experts have reviewed the NIT and cannot definitively determine whether the NIT satisfies the *Daubert* standard because they cannot examine the source code

used to create the NIT. Further, he reasserts his motion to suppress in light of the government's failure to preserve the source code.

The court held a hearing on the motion on August 3, 2015. At the hearing, Special Agent Steven Smith testified that he investigated child exploitation websites on the Tor network as part of the FBI's cyber squad. Filing No. 257, Hr'g Tr. at 8, 15. He has a bachelor's degree in computer science from Georgia Tech and FBI specialized training in the area of cyber investigation, including investigations involving Windows or Unix, networks, analysis of log files, as well as specialized child exploitation investigative training and industry-recognized certifications, such as Network+, Microsoft Certified Systems Engineer, Cisco Certified Network Associate, among others. *Id.* at 12-13. He also trains others in the investigation of online crime, including child exploitation. *Id.* at 13.

He stated that he is familiar with the Tor anonymity network, which achieves anonymity for users, and with the methods and tactics that can be used to subvert that anonymity. *Id.* at 14-15. He explained that the Tor network is a system that enables users to browse the Internet anonymously without revealing their true IP address. *Id.* It is made up of volunteers around the world who install Tor software that turns their computers into what are known as Tor nodes and a collection of Tor nodes comprise the Tor network. *Id.* at 16. Communications are routed through numerous nodes that can be located in any country in the world. *Id.* at 15, 22. Smith identified Government Exhibit 2 as an exhibit that explains how the Tor network operates and how a user uses the Tor network and accesses websites for hidden services. *Id.* at 17-18. He testified that the Tor network is a "proxy system," which means that "instead of proxying through

one computer, it proxies or traffics through three Tor nodes before accessing the Internet." *Id.* at 26.

He further stated that typically, if a website is seized, law enforcement officers are able to use the IP logs on the website to trace back to the users accessing the website. *Id.* at 20. In the case of a Tor hidden service, however, once a website is seized, law enforcement does not know the true IP address of the users, and are not able to trace back who those users are. *Id.* at 21. He stated that in order to identify users, additional investigative tactics or techniques, such as a Flash application "used to cause the user's computer to communicate with an FBI-controlled computer outside of the Tor network," are necessary. *Id.*

Smith testified that he was the lead technical agent in the investigation of websites run by Aaron McGrath out of Omaha, Nebraska. *Id.* at 22. Details connected to the investigation are set out in his affidavit in support of a NIT search warrant. *See* Gov't Ex. 1. Pursuant to the search warrant, the NIT was authorized to collect "the activating computer's actual IP address, the date and time that the NIT determined the IP address; the unique session identifier that was sent by the website; as well as the type of operating system running on the computer, including the type, version, and architecture of the operating system." *Id.* at 24.

Smith is familiar with the NIT technique that was used to identify the defendant in this case. *Id.* at 25. He stated the source of the technique was a website known as "Decloak.net." *Id.* The website was a public website available to anyone. *Id.* at 26. The FBI did not develop the technique. *Id.* at 26. Declaok.net provided a compilation of different methods and techniques that would reveal the user's true IP address

regardless of the user's proxy configuration on their computer. *Id.* at 25. The technique used in this case involved a flash application to identify the activating computer URL. *Id.* at 26. A Flash application is a common web application that is used on many websites—advertising banners on websites are commonly Flash-based applications. *Id.* Smith testified that in 2012, the Flash application functioned to ignore the proxy settings of the activating computer—"it would not route the connection through Tor, it would go directly out of the user's IP address to wherever it was trying to connect to." *Id.*

The Decloak.net website was compiled by HD Moore and was known and published on the website since at least 2008. *Id.* at 27. Smith identified Exhibit 3 as a printout of the decloak.net website as preserved on the "Wayback Machine" of the website "Archive.org" on August 16, 2012. *Id.* The "Wayback Machine" is a tool on the Archive.org website that archives web pages to allow users to historically view those websites at different points in time. *Id.* On August 16, 2012, the decloak.net website listed eight network investigative techniques. *Id.* at 27-28. Technique number five, the Flash application, pertains to this case. *Id.* The technique is described as follows: "When the Flash plugin is installed, it allows direct TCP connections back to the originating host. These connections may bypass the proxy server, leaking the real external address of the user's workstation." *Id.* at 28. The Decloak.net flash application contains a link to a sample code for the technique. *Id.* The sample code had to be configured to deploy the Flash application in conformity with the actions authorized in the search warrant, that is, to collect the IP information, the operating system, the architecture, and the session ID of the computer. *Id.*

Smith stated that an FBI contractor, Matt Edman, helped Smith configure the investigative technique and prepare it for deployment. *Id.* at 29. Edman tested the technique and determined that it worked as designed. *Id.* There was no indication that the technique returned false positives. *Id.* at 30.

Smith testified that after the NIT was deployed, he observed the logs and database results and determined that the NIT was returning appropriate and expected information. *Id.* He stated there did not appear to be any additional functionality built into the code to return anything other than what it was authorized to return. *Id.* He also testified there was no functionality built in that would have planted child pornography on a user's computer. *Id.*

Smith also testified that the servers involved in the investigation were preserved and was made available to the defendant's experts. *Id.* at 38. The servers contained the compiled network investigative technique code. *Id.* at 38. Smith stated he was familiar with the defendant's request for the "source code." *Id.* at 39. He explained that the "source code" would be the "human-readable structured programming language that developers use to create the functions in the events they want to occur." *Id.* at 38-39. "That code is then passed through a compiler and turned into, in this case, ActionScript Bytecode and the Flash application that the computer then uses to execute those actions or functions." *Id.* at 39.

Smith also testified that before the operation went live in November to December 2012, the uncompiled source code was on a computer used by FBI contractor Matt Edman. *Id.* at 40. Smith stated he has undertaken efforts to locate the uncompiled source code but has been unsuccessful. *Id.* at 40-41. He also testified he never

instructed anyone to deliberately or intentionally destroy that uncompiled source code. *Id.* at 41.

Smith also testified it was not necessary to have the uncompiled code to test the functionality of the NIT and explained how to do so. *Id.* at 41-42. He stated he reviewed the defendant's experts' reports and found the experts "used a virtual machine or sandboxing environment to test portions of the configuration of the TB2 server, collection server, and defendant computer environment" and "used our compiled Flash application and ran it in that environment to observe what it did when it was executed." *Id.* at 42-43. Defendant's experts found that the NIT technique was repeatable and reliable and Smith agreed with their conclusion. *Id.* a 43.

In response to speculation that other functionality had been built into the NIT, he stated that the question could be answered without the source code because the Flash application was a straightforward, simple application and "[y]ou can take the compiled Flash application and disassemble it." *Id.* He personally engaged in a disassembly analysis of the compiled code and was able to review the code and observe the functions that were being executed within the Flash application. *Id.* at 44. He "did not observe anything extra that the Flash application was performing, no extra functionality that we were not aware of." *Id.* at 44-45. His results were provided to defense counsel. *Id.*

Further, Smith testified that he determined that the defendant's experts had engaged in a decompilation of the NIT code using a JPEXS decompiler to determine functionality. *Id.* at 46. He performed the same decompilation and did not observe any

additional functionality. *Id.* at 46. He stated defendant's experts concluded that the lack of having the source code would not change the outcome of their report. *Id.*

Dr. Matt Edman also testified at the hearing. Id. at 84-101. In the Fall of 2012 he was employed by the Mitre Corporation as a senior cyber security engineer assigned to the FBI's Remote Operations Unit. *Id.* at 84. He testified he has a bachelor of science degree in computer science from Baylor University and a Master's Degree and Ph. D. in computer science from Rensselaer Polytechnic Institute. *Id.* at 85. He essentially corroborated Smith's testimony. *Id.* at 85-89. He stated he adapted and configured the application found on Decloak.net to collect the limited set of information from a user's computer (a unique identifier, the user's operating system type, version, and architecture) and then send that information to the FBI-controlled server. *Id.* at 89. He wrote the source code and called it "Cornhusker." *Id.* at 87. He stated there was no other functionality installed. *Id.* He further testified he did not plant porn on anyone's computer. *Id.*

He stated that a few months after the investigation in November 2012, he burned the code to a CD and gave it to FBI employee John Solano. *Id.* He returned computers to the used property manager and digital media to John Solano. *Id.* at 88.

He also tested the NIT and his testing did not identify any additional functionality. *Id.* at 88. He stated that it is possible to get back to the uncompiled code from the compiled code through two methods: (1) disassembly—which takes the compiled Flash binary and produces a human-readable list of the individual instructions or op codes contained in that Flash application, and (2) decompilation—which produces a higher

level of the source code that is more easy for humans to understand. *Id.* at 88-89. Both methods could determine that no additional features were built in. Id. at 89.

Michael Pilapil also testified at the hearing. He is a Special Agent with the Operational Technology Division of the FBI. He assists field offices with technical investigational matters. *Id.* at 102. He stated he worked in the same office space as FBI contractor Matt Edman in late 2012 and early 2013. *Id.* at 104. He stated that the contract with Mitre Corporation ended in June 2013. *Id.* at 104. The computer hardware used by Edman was turned in to the property manager in June 2013. *Id.* at 105. He stated it was the normal practice for the users of machines or hardware to return the computers to a "factory state," that is, a reset or a wipe—to reduce data spillage to the next user. *Id.* He further testified that Edman's digital media was turned over to another FBI employee, John Solano. *Id.* at 106. Pilapil described efforts by Solano and himself to locate the digital media that Edman had turned over to Solano. *Id.* at 107-110. Despite those efforts, no source code was found. *Id.* at 110. He also testified that he was not aware of any action to deliberately destroy the uncompiled source code. Id. at 110. Further, he stated that in 2012 there was no central code repository for publicly sourced code that was used in criminal cases, but there is now. *Id.*

The defendant's expert, Matthew Miller, Ph.D., also testified. *Id.* at 130-159. He was employed at Dakota State University, but accepted a position at University of Nebraska at Kearney commencing on August 17, 2015. *Id.* at 130. He teaches computer science and cyber security. *Id.* He testified that he has a bachelor's degree from University of Nebraska at Kearney and a Masters and Ph.D. in Computer Science

from Kansas State University. *Id.* at 131. He was contacted by defense counsel in December 2014. *Id.* He testified he examined the NIT, together with Dr. Ashley Podhradsky and Josh Stroschein. *Id.* at 131. Dr. Podhradsky has a Ph.D. in information systems and is a forensic analyst. *Id.* at 131-32. Josh Stroschein has a Master's degree. *Id.*

He testified that he and his team reviewed the reliability of the NIT. *Id.* at 132. They went to the FBI on two occasions and examined three servers. *Id.* at 132, 144. They decompiled and recompiled the SWF file (the binary code that actually ran on visitor's computers), which was a flash application. *Id.* at 132. He stated the same SWF file was on all three servers. *Id.* at 133. On their second visit to the FBI they verified the results of the first visit and did the reverse engineering, and then verified that the SWF generated from the decompiled source worked on the Cornhusker server. *Id.* at 133.

He stated that the significance of the original source code was that there would be a more verifiable method of verifying that the actual binary that was sent to the computers originally came from that source code and without it, there is less certainty as to whether or not that was the only code that was run. *Id.* He explained that " it is possible to—to modify binary things—binary objects that are run on computers such that they do different— they have different behavior than what you might see from using a—a decompiler or a disassembler." *Id.* at 134. He stated he “would have had more certainty in—in [the team's] verification." *Id.* at 135. He concluded that the NIT was reliable in that "[i]f a user had visited to the TB2 website, it would have reliably returned the IP address of that user to the Cornhusker server." *Id.*

As far as repeatability, he stated they were not able to fully repeat what had happened because they did not have the original source code. *Id.* He stated he was not able "to recompile it in the exact same way" to definitively verify that there was no additional functionality. *Id.* at 136. He testified that there could be a possibility that there was additional functionality. *Id.*

Dr. Miller also testified that he agreed with the conclusion in the expert report that the NIT was reliable and repeatable and agreed that " the NIT determined that it was a Linux machine using a rekonq browser that accessed TB2 from the defendant's IP address." *Id.* at 145. He also stated that his team concluded that not having a source code did not impact their conclusions. *Id.* at 148. He testified they "were able to create—recreate the environment. And when [they] tested it, it did what we would have believed from the source code." *Id.* at 149. However, he stated he would be "more certain" of the analysis if they had been given the source code. *Id.* at 149. His investigation did not disclose any information that would call into question Smith's and Edman's testimony that no additional functionality was built in to the NIT. *Id.* at 150.

Miller presented three scenarios in which a false IP address could be produced: a situation where someone used Cottom's computer as a proxy computer and they proxied all of their connections through it; if somebody had compromised Cottom's computer and was using his computer as a browser; and if somebody had detected that this NIT was in place on the TB2 server and placed an IFrame on another page that Cottom would view, then his computer would have connected to the server and reported back his IP address. *Id.* at 152-53. He also stated that reviewing the source code would not help him determine if a false IP address had been returned. *Id.* at 156.

Reviewing the defendant's computer would help in that determination, but that was not done in this case. *Id.* at 155. He found no evidence that something like that actually occurred in this case. *Id.* at 156.

II. LAW

Federal Rule of Evidence 702 governs the admissibility of expert testimony and requires that: (1) the evidence must be based on scientific, technical or other specialized knowledge that is useful to the finder of fact in deciding the ultimate issue of fact; (2) the witness must have sufficient expertise to assist the trier of fact; and (3) the evidence must be reliable or trustworthy. *Kudabeck v. Kroger Co.*, 338 F.3d 856, 859 (8th Cir. 2003). Expert testimony assists the trier of fact when it provides information beyond the common knowledge of the trier of fact. *Id*. at 860. When faced with a proffer of expert testimony, trial judges are charged with the "gatekeeping" responsibility of ensuring that all expert evidence admitted is both relevant and reliable. *Kumho Tire Co. v. Carmichael*, 526 U.S. 137, 147 (1999); *Daubert v. Merrell Dow Pharms*., 509 U.S. 579, 589 (1993); *United States v. Wintermute*, 443 F.3d 993, 1000 (8th Cir. 2006). A trial court is given wide latitude in determining whether an expert's testimony is reliable. *See Kumho Tire,* 526 U.S. at 152.

Proposed expert testimony must meet three prerequisites in order to be admitted under Rule 702. First, evidence based on scientific, technical, or other specialized knowledge must be useful to the finder of fact in deciding the ultimate issue of fact; second, the proposed witness must be qualified to assist the finder of fact; and third, the proposed evidence must be reliable or trustworthy in an evidentiary sense. *Lauzon v. Senco Prods., Inc.*, 270 F.3d 681, 686 (8th Cir. 2001) (noting district court's gatekeeper

role when screening expert testimony for relevance and reliability). Expert testimony assists the trier of fact when it provides information beyond the common knowledge of the trier of fact. *Kudabeck,* 338 F.3d at 860. The district court's gatekeeper function applies to all expert testimony, not just testimony based in science. *Id.*

Under *Daubert*, district courts apply a number of nonexclusive factors in performing this role. *Lauzon*, 270 F.3d at 686-87. These are: whether the theory or technique can be and has been tested; whether the theory or technique has been subjected to peer review and publication; the known or potential rate of error; whether the theory has been generally accepted; whether the expertise was developed for litigation or naturally flowed from the expert's research; whether the proposed expert ruled out other alternative explanations; and whether the proposed expert sufficiently connected the proposed testimony with the facts of the case. *Id.* at 686-87. "This evidentiary inquiry is meant to be flexible and fact specific, and a court should use, adapt, or reject *Daubert* factors as the particular case demands." *Unrein v. Timesavers, Inc.*, 394 F.3d 1008, 1011 (8th Cir. 2005).

The proponent of expert testimony bears the burden of providing admissibility beyond a preponderance of the evidence. *Lauzon*, 270 F.3d at 686. When the application of a scientific methodology is challenged as unreliable under *Daubert* and the methodology itself is otherwise sufficiently reliable, outright exclusion of the evidence is "warranted only if the methodology was so altered by a deficient application as to skew the methodology itself." *United States v. Gipson*, 383 F.3d 689, 697 (8th Cir. 2004) (brackets omitted) (quoting *United States v. Martinez*, 3 F.3d 1191, 1198 (8th Cir. 1993)). "'Nothing in Rule 702, *Daubert*, or its progeny requires that an expert resolve an

ultimate issue of fact to a scientific absolute in order to be admissible.'" *United States v. Two Elk*, 536 F.3d 890, 904 (8th Cir. 2008) (quoting *Kudabeck,* 338 F.3d at 861). A lack of certainty goes to the weight to be assigned to the testimony of the expert, not its admissibility. *United States v. Brady*, 595 F.2d 359, 363 (6th Cir. 1979).

In the Eighth Circuit, "cases are legion that, correctly under *Daubert*, call for the liberal admission of expert testimony." *Johnson v. Mead Johnson & Co., LLC*, 754 F. 3d 557, 562 (8th Cir. 2014). District courts are admonished "not to weigh or assess the correctness of competing expert opinions." *Id.* Rather, expert testimony should generally "be tested by the adversary process with competing expert testimony and cross-examination, rather than excluded by the court at the outset." *Id.* Any "'doubts regarding whether an expert's testimony will be useful should generally be resolved in favor of admissibility.'" *United States v. Finch*, 630 F.3d 1057, 1062 (8th Cir. 2011) (quoting *Sphere Drake Ins. PLC v. Trisko*, 226 F.3d 951, 954 (8th Cir. 2000)). A "jury, not the trial court, should be the one 'to decide among the conflicting views of different experts.'" *Johnson*, 754 F.3d at 564 (quoting *Kumho Tire*, 526 U.S. at 153).

In a case involving the alleged spoliation of evidence, "a district court is required to make two findings before an adverse inference instruction is warranted: (1) 'there must be a finding of intentional destruction indicating a desire to suppress the truth,' and (2) '[t]here must be a finding of prejudice to the opposing party.'" *Hallmark Cards, Inc. v. Murley*, 703 F.3d 456, 460 (8th Cir. 2013) (quoting *Stevenson v. Union Pacific R.R. Co.,* 354 F.3d 739, 746, 748 (8th Cir. 2004)). Because of the gravity of an adverse inference instruction, "which 'brands one party as a bad actor,'" a district court must issue explicit findings of bad faith and prejudice prior to delivering an adverse inference instruction.

*Hallmark Cards,* 703 F.3d, 461 (quoting *Morris v. Union Pac. R.R.*, 373 F.3d 896, 900 (8th Cir.2004)

III. DISCUSSION

The court finds the defendant's motion in limine to exclude the testimony of the government's experts should be denied. The government has satisfied the three prerequisites under *Daubert*: (1) the testimony of the experts is based on scientific, technical or other specialized knowledge that is useful to the finder of fact in deciding the ultimate issue of fact; (2) the witnesses have sufficient expertise to assist the trier of fact; and (3) the evidence is reliable and trustworthy. The experts have sufficient training, experience, education, and technical expertise to assist the trier of fact. There has been a sufficient showing that the methods and techniques are scientifically reliable.

The government's failure to preserve and produce the original source code, though unfortunate, is of little consequence to this determination. The government's experts and the defendant's own expert all testified that source code information would make little difference in determining that the NIT employed in this case is reliable and that the techniques that were used to derive it are repeatable. The evidence adduced at the hearing shows that the compiled code was maintained and preserved and the original source code can essentially be reverse-engineered from that evidence.

The evidence establishes that the defendant's experts examined the binary code on the mirror image of the server and were able to pull up the binary code for the Flash drive NIT, decompile it to a source code, and recompile it to a new binary code. In essence, they were able to recreate the NIT and to establish that it worked. The

defense expert's testimony establishes that the binary code is likely to correctly identify a requesting computer's correct IP code, rather than to the IP address of a Tor node.

The government has shown that the NIT is capable of being tested and has been tested and has produced reliable results. Both Smith and Dr. Edman testified that no additional functionality was added to the NIT. The court credits that testimony. Defendant's expert agrees that there is no reason to doubt that testimony.

Although the defendant has produced evidence that there are possible scenarios wherein a false IP address could be generated, there is no evidence of any such events occurring in this case. The defendant's expert testified that review of the source code would have added a level of certainty to his analysis, but scientific evidence need not be shown to a level of absolute certainty to be admissible.

To the extent the defendant's motion can be interpreted as a request for an adverse inference instruction, the court finds that there has been no showing of either bad faith or prejudice necessary to warrant an adverse inference instruction. The defendant's own experts stated that availability of the source code would not affect their conclusions. There is no evidence of anything other than an inadvertent failure to preserve the source code. It appears to the court that the government agents/contractors did not go to great length to preserve the publicly-available source code because they did not perceive the source code was important as evidence in view of the fact that the compiled code on the servers had been preserved. Nonetheless, the court is concerned that appropriate procedures were not in place to preserve the source code. The court is also concerned that other courts may read this opinion as justification for future inadvertent failure to preserve all relevant digital data. However,

the testimony demonstrates that evidence preservation in electronic data collection cases is a relatively recent and evolving process. In this instance, the failure appears to be inadvertent and the lost data is essentially recoverable. The government is forewarned that this court is not inclined be so tolerant in the future.

In light of the foregoing, the government has established probable cause for a search warrant and the defendant's renewed motion to suppress will be denied. Accordingly,

IT IS ORDERED that:

1. The defendant's motion in limine (Filing No. 215) and renewed oral motion to suppress are denied.

Dated this 22nd day of December, 2015

BY THE COURT:

s/ Joseph F. Bataillon
Senior United States District Judge